

Remarks

In the office action mailed March 29, 2005, the Examiner rejected claims 1-39 as anticipated by Minear (U.S. Patent No. 5,983,350) under 35 U.S.C. § 102(e). In an advisory action mailed June 21, 2005, the Examiner maintained the rejection.

Applicants have amended the claims and respectfully request that the Examiner reconsider the rejections in light of the amendments and the reasons set forth below.

I. Amendments to the Claims

Currently pending in this application are claims 1-2, 4-10, 12-35 of which claims 1, 2, 9, 14, 20, 28, and 34 are independent and the rest are dependent. Each independent claim has been amended to particularly point-out features of Distributed Network Address Translation (DNAT) with security as it is implemented in the present disclosure.

Independent claim 9, for instance, now includes the following limitations:

wherein the second network device has a publicly routable address, and

wherein the second network device's publicly routable address in combination with the one or more locally unique security values are used to uniquely identify the first network device during secure communications with a third network device on a second external network, and

wherein the secure communications include the one or more locally unique secure values, and

wherein the second network device routes secure communication data from the third network device to the first network device in response to the one or more locally unique security values.

Amendment to claim 9.

Dependent claim 7 has also been amended to point out that that a combination of the second network device's publicly routable address in combination with the one or more locally unique ports of the first network device are "used to uniquely identify the first network device" "prior to establishing a secure connection."

Claims 3, 11, and 36-39 have been cancelled.

II. The “D” in DNAT Stands For “Distributed”

Distributed Network Address Translation or DNAT¹ is a form of network address translation that pushes translation functionality from the network router to the local devices in an internal network.

Prior art network address translation (NAT) involved a router manipulating IP addresses and port numbers within routed packets – converting global addresses to local addresses and *vice versa*. Thus, prior art NAT typically needs to modify an IP packet – thus violating certain specific principles of common security protocols.

DNAT, on the other hand, distributes the function of address translation to the local endpoint. In the claimed invention, this local endpoint is described as the “first network device.” In first-generation DNAT, a local port is allocated to the first network device by a second network device (e.g., a router). A unique ID for the first network device can be created by the combination of a public address of the second network device and the local port allocated to the first network device. Thus, for incoming messages, the router can simply decode the addressee information by consulting a port allocation table to determine the location of the first network device and forward the message to the first network device.

The principles of DNAT thus allow for network translation without modifying packets mid-stream and without adding significant processing burden on the router.

¹ An old form of network address translation known as dynamic NAT also uses the acronym DNAT.

III. DNAT with Security

The present invention offers a further advance on DNAT by adding security functionality – thus creating the possibility of creating a secure (virtual) connection using DNAT. DNAT with security allows a router to direct incoming secure messages to the first network device without altering the message content, and with only a small processing burden on the router. And, unlike traditional NAT, the present disclosure is not limited to firewall-to-firewall security. *See, for example*, Minear, Column 1, lines 50-51.² The prior art is also incapable of DNAT with security because security configurations will not allow a router to manipulate IP or Port addresses without first decrypting the message. Minear's use of the router/firewall to securitize and modify packets becomes clear in its discussion of Figure 2. Figure 2 is a figure of a router/firewall 18 that encrypts and decrypts messages:

In the embodiment shown in FIG. 2, an SADB Master copy 52 is maintained in persistent memory at application layer 48 while a copy 54 of SADB is maintained in volatile memory within the kernel. If the message is supposed to be encrypted, the message is decrypted based on the algorithm and key associated with the particular SA and the message is transferred up through transport layer 46 to proxy 50. Proxy 50 examines the source and destination addresses and the type of service desired and decides whether authentication of the sender is warranted. If so, proxy 50 initiates an authentication protocol.

Minear, Column 6, lines 6-18.

A feature of the claimed invention is that the router (second network device) can maintain a port allocation table that associates the port(s) of the first network device with the security value(s) allocated to the device. Using the table, an incoming message that

² Minear does disclose firewall-to-workstation encryption in Figure 5 and at Column 12, lines 49-63, however, this appears to be limited to situations where there is no router or LAN – and thus no need for network address translation.

includes an IP address of the router and the security value(s) will be uniquely identified with the first network device and routed properly. This routing can be done without decrypting or altering the secure communication.

Each of the independent claims have been amended to specifically point out that the combination of the locally unique security value(s) associated with the first network device in combination with the router's public address can be used to uniquely identify the first network device, and to indicate that the router will route a secure communication to the first device based on the secure communication including the locally unique security value(s). The prior art references, including Minear, do not disclose this routing based on the security parameters – i.e., a system that allows for what we term DNAT with security. In this way, the router can direct secure communications to a local device without decrypting or otherwise altering the communication.

Minear also fails to disclose a first network device requesting and receiving locally unique security values from a second network device, an integral part of DNAT with security as claimed. (See, e.g., **claim 1** of the present application). Minear does note that: "Users that already have IPSEC available on their own host machine will, however, have to request that the firewall administrator set up SA's in the SADB for their traffic." Minear, Col. 6, lines 27-31. However, creating an entry in a database, as disclosed by Minear, is quite different from requesting a security value and receiving it at the local computer as claimed. In fact, Minear's method of retaining control of the SADB at the router/firewall level is a reflection of the Minear's router/firewall control, the antithesis of distributed NAT. Further, in Minear, the security values are all stored in the SADB on

the router – there is no disclosure for storing security values on a local device (first network device) as in claim 1 of the present application. Specifically, claim 1 calls for:

storing the one or more locally unique security values on the first network device, wherein the one or more locally unique security values are used to create a secure virtual connection for secure communications between the first network device and the third network device, wherein the secure communications include the one or more locally unique secure values, and wherein the second network device routes secure communication data from the third network device to the first network device in response to the one or more locally unique security values. ~~and for distributed network address translation.~~

Because Minear does not disclose this storing step, it cannot anticipate claim 1.

Dependent **claim 7** further includes limitations that take advantage of this traditional DNAT form. In claim 7, prior to establishing a secure connection, a local port value is used to identify the first network device (because there may be no security values in the communications yet). Claim 7 specifically calls for the first device requesting one or more locally unique ports used to uniquely identify the first network device. Again, this additional feature is not disclosed by Minear. (Note, independent claim 34 has a parallel limitation).

In addition, independent **claim 9** includes the step of sending the one or more locally unique security values in a response message with the first protocol to the first network device. Because Minear maintains all control at the router level, the reference simply does not disclose this step. (Note, independent claims 14 and 34 have parallel sending limitations).

IV. Conclusions

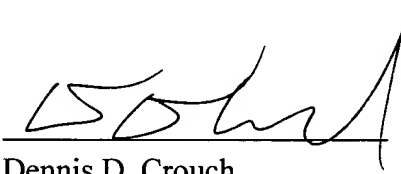
Each claim, as amended, includes elements that are not disclosed by the cited references, and thus not anticipated. Applicant would also submit that, because Minear

maintains control of the security sessions at the router/firewall level, Minear would not be properly applied in an obviousness-type rejection.

Applicant therefore respectfully asks the Examiner for reconsideration and for a speedy allowance.

Respectfully submitted,

Date: SEPT 29 2005

By: 
Dennis D. Crouch
Registration No. 55,091